Claims

[c1] 1. A method for protecting the configuration of a securable object in an operating system from members of a locally privileged group, wherein a security descriptor for the securable object includes a discretionary access control list (DACL), the method comprising:

making a copy of the security descriptor;

adding a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object; and

overwriting the security descriptor in the operating system with said copy.

[c2] 2. The method of claim 1, further comprising:

determining the relative identifier (RID) of the securable object; and

finding the security descriptor for the securable object based on said RID.

[c3] 3. The method of claim 1, further comprising examining the DACL to discover whether said access right is already denied.

[c4] 4. The method of claim 1, wherein said new ACE is added as the first ACE in the DACL.

[c5] 5. The method of claim 1, wherein the securable object is a group other than the local administrators group.

[c6] 6. The method of claim 5, wherein said group is a domain administrator group.

[c7] 7. The method of claim 6, wherein said domain administrator group is a remotely hosted group, and the method further comprising adding said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object.

[c8] 8. The method of claim 5, wherein said access right includes a right to change permissions of said group.

[c9] 9. The method of claim 7, wherein said access right also includes a right to view permissions of said group.

[c10] 10. The method of claim 1, wherein a single software tool performs the method.

[c11] 11. A computer program, embodied on a computer readable storage medium, for protecting the configuration of a securable object in an operating system from members of a locally privileged group, wherein a security descriptor for the securable object includes a discretionary access control list (DACL), the computer program comprising:

a code segment makes a copy of the security descriptor;

a code segment that adds a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object; and

a code segment that overwrites the security descriptor in the operating system with said copy.

[c12] 12. The computer program of claim 11, further comprising:

a code segment that determines the relative identifier (RID) of the securable object; and

a code segment that finds the security descriptor for the securable object based on said RID.

[c13] 13. The computer program of claim 11, further comprising a code segment that examines the DACL to discover whether said access right is already denied.

[c14] 14. The computer program of claim 11, further comprising a code segment that provides that said new ACE is added as the first ACE in the DACL.

[c15] 15. The computer program of claim 11, wherein the securable object is a group other than the local administrators group.

[c16] 16. The computer program of claim 15, wherein said group is a domain administrator group.

[c17] 17. The computer program of claim 16, wherein said domain administrator group is a remotely hosted group, and said code segment that adds further adds said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object.

[c18] 18. The computer program of claim 15, wherein said access right includes a right to change permissions of said group.

[c19] 19. The computer program of claim 18, wherein said access right also includes a right to view permissions of said group.

[c20] 20. The computer program of claim 11, wherein all said code segments are part of a single software tool.

[c21] 21. A system for protecting the configuration of a securable object in an operating system of a computer from members of a locally privileged group, wherein a security descriptor for the securable object includes a discretionary access control list (DACL), the system comprising:

means for making a copy of the security descriptor;

means for adding a new access control entry (ACE) to the DACL in said copy, wherein said new ACE specifies denying the locally privileged group an access right to the securable object; and

means for overwriting the security descriptor in the operating system of the computer with said copy.

[c22] 22. The system of claim 21, further comprising:

means for determining the relative identifier (RID) of the securable object; and

means for finding the security descriptor for the securable object based on said RID.

[c23] 23. The system of claim 21, further comprising means for examining the DACL to discover whether said access right is already denied.

[c24] 24. The system of claim 21, further comprising means for providing that said new ACE is added as the first ACE in the DACL.

[c25] 25. The system of claim 21, wherein the securable object is a group other than the local administrators group.

[c26] 26. The system of claim 25, wherein said group is a domain administrator group.

[c27] 27. The system of claim 26, wherein said domain administrator group is a remotely hosted group, and said means that adds further adds said new ACEs to the DACL in said copy to deny all local groups said access right to the securable object.

[c28] 28. The system of claim 25, wherein said access right includes a right to change permissions of said group.

[c29] 29. The system of claim 28, wherein said access right also includes a right to view permissions of said group.

[c30] 30. The system of claim 21, wherein said means are comprised within a single software tool.